FIT4DORA

DORA (DIGITAL OPERATIONAL RESILIENCE ACT)
Am 16.01.2023 in Kraft getreten, **Anwendung ab dem 17.01.2025.**
Als EU-Verordnung gilt DORA ohne weitere Umsetzungsakte unmittelbar in den Mitgliedsstaaten.

Die Gründe und die Ausgangslage

- Obwohl die Anzahl an Cyberattacken erheblich zugenommen hat und die gestiegenen IKT-Risiken bekannt sind, gab es auf EU-Ebene bislang für Finanzunternehmen und IKT-Drittdienstleister keine einheitlichen Regelungen zur Stabilisierung der digitalen operationellen Resilienz.

Der Kreis der betroffenen Akteure

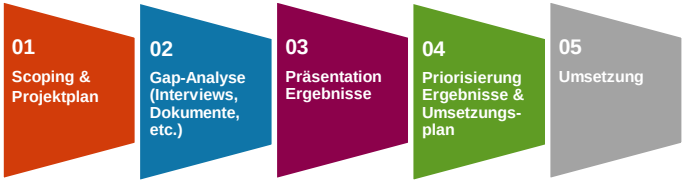
- EU-Finanzunternehmen
- IKT-Drittdienstleister
- (Europäische) Aufsichtsbehörden (BaFin, EBA, EIOPA, ESMA).

Die Ziele von DORA

- Erhöhung der Widerstandsfähigkeit des Finanzsektors gegen IKT-Risiken
- Minimierung von Cyberrisiken
- Sicherstellung der Wirksamkeit von Präventions- und Resilienzmaßnahmen
- Zugang Finanzaufsicht zu Informationen über IKT-Vorfälle
- Etablierung Informationsaustausch zu Cyberbedrohungen im Finanzsektor
- Verbesserung IKT-Risikomanagement

Die Umsetzung

Durchführung FitnessCheck DORA



Ihre Ansprechpartner

Luther.
Nicole Bittlingmayer
Mail nicole.bittlingmayer@luther-lawfirm.com

Knowledge River Enterprise IT Resilience Optimization
Sven Bittlingmayer
Mail Sven.Bittlingmayer@KnowledgeRiver.com

VIVACIS Consulting
Anna Schäfer
Mail anna.schaefer@vivacis.de

FIT4DORA

DORA erfordert interdisziplinäre Anwendungskompetenz: Tiefes juristisches Know-how, intensive Erfahrung mit regulatorischen Transformationsprozessen, hohes Verständnis von technischem IT-Betrieb bzw. -Management, Zusammenarbeit von eingespielten Akteuren in fraktionierten, aufsichtsrechtlich geprägten Strukturen.

Governance

- Überprüfung, Anpassung bzw. Erstellung der Dokumentation des internen Governance- und Kontrollrahmens im Hinblick auf Cyber- und IKT- Sicherheitsrisiken (Rahmenanweisung DORA).
- Schulung und Fortbildung hinsichtlich DORA.
- ...

IKT-Risiko-management

- Überprüfung der Dokumentation zum IKT-Risikomanagementrahmen (insb. Strategie, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle).
- Maßnahmen zur Erkennung IKT-bezogener Vorfälle.
- IKT-Notfallmanagement.
- Bereitstellung ausreichender Kapazitäten und Ressourcen.
- ...

Regelungen für Tests

- Durchführung Systemtests in regelmäßigen Abständen; mindestens einmal pro Jahr.
- Automatisierte Aufbereitung Ist-Zustand IT (Topologie, Konfiguration), in verschiedenen Detailgraden unterschiedliche Bedrohungsszenarien zu berücksichtigen.
- Lösung zur teilautomatisierten Erstellung von Dokumentationen basierend auf gesammelten Daten und aufbereiteten Informationen: IT-Infrastruktur, DORA, Pen-Test-Vorbereitung und Durchführung.
- ...

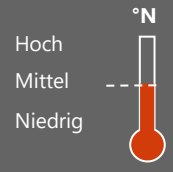
IKT-Berichterstattung

- Definition Frühwarnindikatoren für IKT-Vorfälle.
- Implementierung Risikomanagement-prozess für IKT-Vorfälle.
- Klassifizierung möglicher Vorfälle bzw. Störungen in der standardisierten Berichterstattung.
- ...

Risiko-Management IKT-Drittanbieter

- Review Due Diligence IKT-Drittparteien (Auswahl, Geeignetheit), Prüfung (Unter-)Auslagerungs-Vertragsdokumentation mit IKT-Dienstleistern.
- Anpassung/ Verhandlung Verträge (unter Berücksichtigung IT-rechtlich zu beachtender Aspekte).
- Anpassung/Erstellung Auslagerungsstrategie hinsichtlich DORA.
- Etablierung Berichtswesen; Prüfung der Berechtigungen auf Dokumente zuzugreifen.
- Durchführung Vor-Ort-Prüfungen; Aussprache von Empfehlungen oder Anweisungen.
- ...

Informationsaustausch



- Erstellung Vereinbarungen zum Informationsaustausch.
- Unterstützung bei Etablierung des Informationsregisters.
- IT-gestützte Vorfallsaufbereitung.
- ...